

CLAIMS

What is claimed is:

- 5 1. A method for obtaining video data, the method comprising:
 - providing a control signal to a video data acquisition system;
 - receiving an output signal from the data acquisition system in response to providing the control signal, the output signal including video data captured by the video data acquisition system; and

10 verifying an authenticity of the video data from the data acquisition system by checking that the received output signal includes modifications according to the control signal.

2. A method as in claim 1, wherein providing a control signal includes:
 - providing a control signal that includes a key for encrypting the video data transmitted by the video data acquisition system.

15 3. A method as in claim 2 further comprising:
 - maintaining confidentiality of the key so that recorded subjects of the video data acquisition system do not have access to the key; and
 - entrusting an escrow agent with knowledge of the key.

20 4. A method as in claim 1, wherein providing a control signal includes:
 - providing a control signal that includes a command to overlay a recognizable pattern onto the video data such that the recognizable pattern appears on a viewing display when the video data is replayed.

25 5. A method as in claim 4, wherein overlaying a recognizable pattern onto the video data includes:

modifying a value of a text string associated with the video data that appears on the display when the video data is replayed at a later time.

6. A method as in claim 1 further comprising:

5 providing a control signal that identifies a hashing function to be used for hashing at least a portion of the video data; and
at least occasionally receiving hashed values associated with portions of the video data in lieu of receiving a substantially continuous stream of corresponding non-hashed video data.

10

7. An apparatus for authenticating video data including a processor that provides a control signal to a video data acquisition system, the processor receiving an output signal from the data acquisition system including video data in response to providing the control signal, the processor verifying an authenticity of the video

15 data from the data acquisition system by checking that the received output signal includes modifications according to the control signal.

8. An apparatus as in claim 7, wherein the control signal includes a key for encrypting the video data transmitted by the video data acquisition system.

20

9. An apparatus as in claim 7, wherein the data acquisition system, in response to receiving the control signal, overlays a recognizable pattern onto the video data such that the recognizable pattern appears on a viewing display when the video data is replayed.

25

10. An apparatus as in claim 9, wherein the recognizable pattern includes a text string that appears on the display when the video data is replayed at a later time.

11. An apparatus as in claim 10, wherein the text string is a clock value.

30

12. A method for maintaining video data, the method comprising:
 - 5 receiving video data from a video data acquisition system;
 - hashing a selected portion of the video data to produce a hash value;
 - storing the selected portion of the video data and corresponding hash value in a first memory storage device; and
 - transmitting the corresponding hash value over a network for storage in a second memory storage device.
- 10
13. A method as in claim 12 further comprising:
 - retrieving the selected portion of video data from the first memory storage device; and
 - verifying an authenticity of the selected portion of the video data by
 - 15 checking that the selected portion of video data, when hashed, produces a same hash value as the corresponding hash value stored in the second memory storage device.
14. An apparatus for maintaining video data, the apparatus comprising:
 - 20 a video data processor that receives video data from a video data acquisition system, the video data being stored in a first memory storage device; and
 - a hashing processor that generates a hash value based on a selected portion of the video data, the hash value being stored in the first memory storage device
 - 25 and a second memory storage device.
15. An apparatus as in claim 14, wherein the selected portion of video data retrieved from the first memory storage device is authenticated by checking that the selected portion of video data from the first memory storage device, when hashed,

produces a same hash value as the corresponding hash value stored in the second memory storage device.

16. A method for generating an output signal from a video data acquisition system,

5 the method comprising:

receiving a video signal that varies depending on sensed images;

encrypting the video signal using a first key;

encrypting the first key using a second key; and

including at least the encrypted first key and encrypted video signal in the

10 output signal.

17. A method as in claim 16 further comprising:

randomly generating a new encryption key for encrypting different

portions of the video signal over time.

15

18. A method as in claim 16 further comprising:

generating the output signal to include multiple tracks, one of the tracks including the encrypted video signal and the encrypted first key, another track including sensor data provided by a sensor associated with the video data

20 acquisition system, the sensor data also being encrypted using an encryption key.

19. A method as in claim 18, wherein generating the other track includes generating encrypted RFID (Radio Frequency Identification) information.

25 20. A method as in claim 16 further comprising:

implementing a recognition algorithm to identify objects associated with the sensed images; and

in response to recognizing an object, embedding encrypted data information identifying the recognized object in the output signal.

30

21. A method for maintaining video data, the method comprising:
 - providing an encryption key to a video data acquisition system;
 - encrypting at least a portion of an output signal generated by the video data acquisition system using the provided encryption key; and
- 5 maintaining confidentiality of the provided encryption key so that recorded subjects of the video data acquisition system do not have access to the provided encryption key, knowledge of the provided encryption key being entrusted to an escrow agent.
- 10 22. A method as in claim 21 further comprising:
 - verifying an authenticity of the output signal by checking that at least a portion of the output signal is encrypted with the provided key.
23. A method as in claim 21 further comprising:
 - 15 notifying the escrow agent to decrypt selected portions of the output signal previously stored in memory using the provided encryption key.
24. A method as in claim 21 further comprising:
 - 20 encrypting video data according to a hierarchical set of keys including the provided encryption key, at least one key of the hierarchical set of keys being used to encrypt another key associated with the output signal.
25. A method as in claim 24 further comprising:
 - 25 using the provided encryption key to encrypt at least one other encryption key associated with the output signal.
26. A method for generating an output signal from a video data acquisition system, the method comprising:
 - 30 receiving a video signal that varies depending on images detected by a video camera;

encrypting a selected portion of the video signal using a first encryption key;

receiving a sensor signal that varies depending on detection of objects in a vicinity of the data acquisition system; and

5 encrypting a selected portion of the sensor signal using a second encryption key; and

producing the output signal to include at least the encrypted video signal and the encrypted sensor signal.

10 27. A method as in claim 26 further comprising:
randomly generating new values of encryption keys to encrypt different segments of the video signal over time.

28. A method as in claim 26 further comprising:
15 generating the output signal to include multiple tracks, one of the tracks including the encrypted video signal and the encrypted first key, another track including sensor data provided by a sensor associated with the video data acquisition system.

20 29. A method as in claim 28, wherein generating the other track includes generating encrypted RFID (Radio Frequency Identification) information.

30. A method as in claim 26 further comprising:
25 implementing a recognition algorithm to identify objects associated with the sensed images; and
in response to recognition of an object associated with the sensed images, embedding encrypted data information identifying the recognized object in the output signal.

30 31. An apparatus to support surveillance, the apparatus comprising:

a camera to generate a video signal that varies depending on sensed images;
a memory device to store at least first and second encryption keys; and
a processor that encrypts the video signal using the first encryption key,
5 the processor encrypting the first encryption key with the second encryption key,
the processor producing an output signal including at least the encrypted video
signal and the encrypted first encryption key.

32. An apparatus as in claim 31 further comprising:

10 an encryption key generator that randomly generates a new value for the
first encryption key to uniquely encrypt different portions of the video signal over
time.

33. An apparatus as in claim 31, wherein the processor generates the output signal to

15 include multiple tracks, one of the tracks including the encrypted video signal and
the encrypted first key, another track including sensor data provided by a sensor
associated with the video data acquisition system that also has been encrypted.

34. An apparatus as in claim 33, wherein the other track includes encrypted RFID

20 (Radio Frequency Identification) information.

35. An apparatus as in claim 31 further comprising:

25 a recognition system to identify objects associated with the sensed images,
the processor embedding encrypted data information identifying the recognized
object in the output signal.

36. An apparatus to support surveillance, the apparatus comprising:

a video camera that generates a video signal that varies depending on
sensed images;

a sensor device that generates a sensor signal depending on detection of objects in a vicinity of the video camera; and

5 a processor in communication with the memory device that encrypts the video signal using a first key and encrypts the sensor signal using a second key, the processor producing an output signal to include at least the encrypted video signal and encrypted sensor signal.

37. An apparatus to support surveillance, the apparatus comprising:

10 a camera to generate a video signal that varies depending on sensed images;

15 a memory device to store at least first and second encryption keys; and means for encrypting the video signal using the first encryption key and means for encrypting the first encryption key with the second encryption key to produce an output signal including at least the encrypted video signal and the encrypted first encryption key.

38. A computer program product including a computer-readable medium having instructions stored thereon for processing data information, such that the instructions, when carried out by a processing device, cause the processing device to perform the steps of:

20 receiving a video signal that varies depending on sensed images;

25 encrypting the video signal using a first key;

 encrypting the first key using a second key, the first and second key being different than each other; and

 including at least the encrypted first key and encrypted video signal in the output signal.